From: Don Jerman
To: Microsoft ATR
Date: 12/23/01 10:21am
Subject: Microsoft Settlement

[Text body exceeds maximum size of message body (8192 bytes). It has been converted to attachment.]

Thank you for your consideration of these comments on the proposed settlement of United States v. Microsoft.

I am a database administrator with more than 12 years in professional service to the State of North Carolina. I have worked in many capacities within our IT organization and I have worked with Microsoft operating system products for the majority of my career. I find that the settlement is probably too lenient to be in the public interest, but with a little strengthening in specific areas, it may serve. Here are the points of weakness that I would like to see addressed, if this settlement is to be entered.

In abstract, the main problem is that the settlement does not protect the consumer, but protects only businesses that consume Microsoft products. Particularly, that an assumption is made that only viable businesses which publish software have a valid interest in API's and communication protocols.

While I recognize that the settlement is the product of a negotiation, it should be noted that Microsoft has been found guilty of violations of the law, and that any settlement must adequately limit their ability to continue to restrain their competitors in an unfair manner. I submit, further, that constraining the ability of private citizens to become competitors falls into this category. Below, I comment on individual sections and paragraphs, preceeding the comments with the reference to the relevant section and paragraph of the Proposed Final Judgment. I refer you especially to the comments regarding III,J, as in my opinion they form a critical weakness in the document, apparently founded on an incorrect appreciation of the nature of computer security.

Here are my comments by section and paragraph:

III,A
Although the settlement requires two warnings before termination of an agreement, and allows instant termination of the agreement upon the third, it does not require that the three warnings be given in good faith, nor does it provide a mechanism for timely review of the claims, merely a 30-day period for remedy by the OEM. Microsoft can use this to stop any agreement it pleases simply by making spurious claims.

III,B,3
The limits on size and appearance of a middleware user interface are not consistent with III,B,1 and III,B,2, and do not serve an obvious purpose other than to allow Microsoft to limit the options of its competitors. The limitations permit Microsoft to minimize their competitors' ability to innovate in this area without regard to the functionality their competitors may be attempting to provide. These limits should be struck from the settlement, and replaced with language similar to III,B,2, which says that differences shall not impact the usability of the operating system.

III,I
For the purpose of licensing or publishing API's and Communications Protocols, "Third Parties" described in III,E and III,I should be construed to be anyone permitted by III,J,2(a), that is, anyone who "has no history of software counterfeiting or piracy or willful violation of intellectual property rights". Businesses are not the only providers of software and services, and with respect to these products, failure to license is failure to permit competition. This is one of the core weaknesses of this document, in my opinion, because as a State agency my organization is none of the entities named, yet we have used Microsoft APIs and communications protocols to build our software.

III,J,1

This is one of the main weaknesses in the document.

III,J,1(a) should be limited to "keys, authorization tokens and enforcement criteria" only, but the API's and Communications Protocols should not be withholdable. Here is my analysis:

Observe that "secret" bugs, APIs and protocols have been compromised regularly by virus-writers in recent years.
For instance Thai hackers have hacked the anti-piracy features of Windows XP, presumably without API documents:
http://www.zdnet.com/zdnn/stories/news/0,4586,5099511,00.html
There is no reasonable expectation that failure to provide documentation will prevent insecure use of these APIs by those who want to abuse them. If the code is published in machine-readable form (as it must be, to be used), then those who do not follow rules will be able to read it and use it, whether a formal API is published or not. Anything readable by a machine is readable by some people, and those people can write their findings in documented form for less-skilled people to use.

Keys, tokens and enforcement criteria are legitimate secrets that must be kept secret to be effective. However, documentation of methods, APIs and communications protocols are useful to those who wish to interact with the system. They are not required to abuse the system, as reverse-engineering will yeild the needed information. But they are required to make legitimate use of the system, as reverse engineering of these methods, APIs and protocols is prohibited by the Digital Millennium Copyright Act, since they may be used to secure access to copyrighted materials. Since the abuse of these systems is likely to be an offense anyway, it its not necessary to restrict the information required for legitimate use.

Allowing Microsoft to keep these items a secret permits them to have an advantage over their legitimate competitors, without significantly retarding the development of attacks against Microsoft systems.

I refer the reader to these excellent discussion of whether secrecy about methods and flaws is desirable or not:
http://www.computerworld.com/storyba/0%2c4125%2cNAV47_STO65969%2c00.html
http://www.counterpane.com/crypto-gram-0111.html
Essentially, they take the position that the vulnerabilities in a system exist whether or not the documentation is published, and will be discovered and exploited whether or not documentation is forthcoming. My conclusion is, therefore, that non-publication merely prevents competition, not abuse. Furthermore that publication can lead to informed decisions, error detection, and intelligent application of precautionary measures, rather than discovery-by-abuse as we've seen before.

III,J,2

This is another of the main weaknesses of the document

III,J,2(a) is perfectly reasonable, and should be left alone.

III,J,2(b) prohibits entities from reviewing the documentation to discover if they have a need for it. As such, and given the arguments under III,J,1 above, III,J,2(b) should be struck from the document. Furthermore, the word Business offers a "handle" for III,J,2(c), to which I object below. The word should be struck if this paragraph is allowed to stand.

III,J,2(c) allows Microsoft to prohibit anyone who is not a Business, by whatever criteria they decide, from accessing these API's. I have

argued under III,J,1 above that such prohibition is not requried, and I now argue that it is harmful to the consumer. If these API's and protocols are required to interact with Microsoft servers, then preventing the private consumer from doing so prevents their contribution to non-commercial entities, and their full use of the product. There is no justification offered why only businesses, and only viable businesses, should have this access.

In any case, permitting Microsoft (and not, say, the TC or USDOJ) to provide the criteria at their sole discretion is absolutely ludicrous!

If anything, the settlement should be forcing more disclosure, and should include all end-users of Microsoft platforms as potential licensees. Furthermore for documentation licenses, the standard for reasonable charges should be related closely to the cost of any required redaction and distribution, as presumably Microsoft needs to produce the documentation for its own use.

III,J,2(d) permits Microsoft to charge any price from anyone using one of these API's, for and unspecified testing procedure. Again, this permits Microsoft to restrain private citizens, nonprofits and businesses with relatively little capital from producing products that might compete with Microsoft products. In my analysis:
1. If the API or protocol is secure, then no product could possibly corrupt or violate the server systems by using it (after all it's perfectly reasonable for the server to refuse any request that would violate security).
2. This test permits Microsoft to analyze competing products prior to release -- a directly anticompetetive act! It offers prior knowledge and time to act to Microsoft whenever a competitor wishes to release an innovative product.
3. Reliability and security testing now resides with the end-user. End users such as my employer have frequently found that Microsoft's testing of its own products leaves much to be desired. What assurance does Microsoft offer that their testing of these third party products will be more useful? This test will not reduce the burden on the end-user, but may reduce their perception of the potential risk (without really reducing the risk), resulting in a less secure world.
4. If, through some extraordinarily poor judgement on the part of the plaintiffs, this paragraph is allowed to stand, then Microsoft should be held liable for subsequent failures of security for any products surviving this test, and furthermore, the TC should be available for appeal should Microsoft fail to approve any competitor's product. Absence of that language makes this paragraph an invitation to restrain competition! In short, if Microsoft is to become a mandatory testing body, they should be unable to disclaim liability for damages caused by failure of their product and the products they test.
5. If the tests are to be performed, a third party should perform the tests, and all relevant Microsoft products should similarly endure the tests and be approved or rejected based on the same criteria that are applied to their competitors. Finally, the competitors must be able to appeal to the TC any discrepancies between the provided documentation and the test results.

I strongly recommend that III,J,2(b,c,d) be struck entirely, or radically altered to provide a real opportunity to all consumers (including non-commercial consumers) to license these materials without providing anticompetetive advantages to Microsoft.

IV
With regard to section IV, my only comment is that the proceedings of the TC should be in the public record, including all documentation and communication between Microsoft, the Plaintiffs and the TC, except where the TC or the Court determines that specific data regarding authentication keys and tokens, trade secrets or future business plans should be redacted or released on a delayed schedule, to protect the viability of Microsoft's business and their business dealings. In such

cases they should be redacted in a manner consistent with existing practise in disclosure of public records, so that the public can know the existence and extent of the redacted material, but not its content. It is my hope that these changes, or changes in this spirit, will be introduced to the Final Judgment. Thank you for your consideration.